

**DOW CORNING**

October 30, 2015

Joseph Foster  
Attorney General  
Office of the Attorney General  
33 Capital Street  
Concord, NH 03301

Re: Dow Corning Corporation Security Incident

Dear Attorney General Foster:

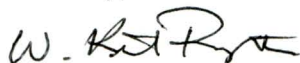
In accordance with the Notice of Security Breach law of New Hampshire, we are providing you with this notice of a security breach.

The incident arose because two contractors of one of our vendors who had access to employee data as a part of their interaction with us took a number of documents upon their termination. The personal information involved included names, contact information, financial information (such as salary information and some bank account numbers), Social Security Numbers and non-HIPAA related benefit enrollment information. The incident occurred between August 31, 2015 and September 30, 2015 and affected 9 residents of New Hampshire who will be notified the week of November 2, 2015 (a copy of which is attached).

Dow Corning continues to work diligently to resolve this incident. We immediately set up a response team to determine who was affected and how, and we are continuing to work diligently with our experts and evaluating all legal options. To assist in the protection of affected individual's personal information, we have partnered with CSID to provide two years of credit protection.

If you have any questions or would like additional information, please feel free to contact me (contact information is provided under my signature).

Sincerely,



W. Kirk Royster  
IT Security Director  
Dow Corning Corporation  
1 East Main Street  
Bay City, Michigan 48708  
(989) 895-8345

STATE OF NH  
DEPT OF JUSTICE  
2015 NOV -2 AM 10:00

November 2, 2015

CSID PIN code: [INSERT]

Xxxx  
Xxxx  
Xxxx,xxxx

Dear xxx,

**Re: Important Notice – Potential Misuse of Personal Identifying Information**

I am writing to inform you about a recent data incident at Dow Corning that included pieces of your personal information.

It is important to stress at this stage that we have no evidence that your information has been used by those who took it or that it has been given or sold to third parties. We take the privacy and security of your information very seriously, and we have taken numerous steps to investigate the incident, mitigate the risks to those affected, and prevent this from happening again. We are conducting a review of current procedures and evaluating enhancements or new procedures.

The incident occurred because two contractors of one of our service providers who had access to employee data as a part of their work took a number of documents upon their termination. Personal information was included in those documents and included names, contact information, financial information (such as salary information and some bank account numbers), Social Security Numbers and non-HIPAA related benefit enrollment information. The incident occurred between August 31, 2015 and September 30, 2015.

To assist in the protection of your personal information, we have partnered with CSID to provide two years of CSID Protector Services, including credit monitoring and identity theft restoration coverage at no cost to you. CSID is a leading provider of identity protection and fraud detection solutions and technologies.

In order to activate your CSID Protector coverage, visit <https://www.csid.com/dowcorning> to complete a **secure** sign up process and answer some questions to confirm your identity. This process begins by submitting the PIN code at the top of this letter. This PIN code can only be used once and cannot be transferred to another individual.

I want to reassure you that at Dow Corning we continue to work diligently on this matter. We immediately set up a response team to determine who was affected and how, and we are continuing to work with our experts and evaluate all legal options. This notice was not delayed by a law enforcement investigation. For additional information, please use the toll-free number provided below. ***You should remain vigilant in reviewing your credit-related statements and information.***

We advise you also to contact any of the major credit reporting agencies to place a fraud alert on your credit report, and to learn about identity theft programs offered by the Federal Trade Commission (FTC). On the following pages you will find details on how to contact the credit reporting agencies and the FTC.

**Please see the remainder of this letter for details on the coverage and instructions on how to complete enrollment in CSID Protector.** Should you have any questions regarding the coverage or the sign up process, please contact CSID Member Services at 855-955-2743, Monday through Saturday, 8AM to 8PM CST, or e-mail [support@csid.com](mailto:support@csid.com).

Thank you for your patience and understanding and rest assured that we are doing everything possible to manage this situation and protect your data.

Sincerely,



Mike Conway  
Dow Corning Corporation  
Senior Vice President, Chief Human Resources Officer



## CSID Protector

After you complete registration for the CSID Protector coverage we are providing for you at no charge, you will have increased visibility into possible fraudulent activity so you can respond more quickly if such activity is detected. You will also have a team of Identity Restoration Specialists to guide you through the recovery process should you become a victim of identity theft, and an insurance policy issued to CSID for up to \$1,000,000 in coverage for certain reimbursable expenses (subject to the terms and exclusions of such policy). We encourage you to complete registration as quickly as possible before January 31, 2016 to take advantage of the CSID Protector coverage we are providing for you at no charge.

The sign-up process is conducted online via CSID's secure website at <https://www.csid.com/dowcorning>. You will need your CSID PIN code shown at the top of the first page of this letter. This PIN code can only be used once and cannot be transferred to another individual. Once you have entered your PIN code, you will be prompted to answer a few security questions to authenticate your identity, including: previous addresses, names of creditors and payment amounts.

Should you have any questions regarding the coverage or the sign-up process, please contact CSID Member Services at 855-955-2743, Monday through Saturday, 8AM to 8PM CST, or email at [support@csid.com](mailto:support@csid.com). Once you have enrolled and created your username and password, you will return to CSID's page to log in and access your personal information on future visits.

### CSID Protector includes:

- **Credit Monitoring:** Monitor your TransUnion credit file for credit inquiries, delinquencies, judgments and liens, bankruptcies, new loans and more.
- **CyberAgent®:** CSID's Internet surveillance technology scours the dark Web, chat rooms and bulletin boards 24/7 to identify trading or selling of your personal information online. CyberAgent® monitoring alerts you to compromised identity details such as Social Security Number, phone number as well as credential information such as email addresses that are often used for online logins.
- **Child Monitoring:** Minors have information that is often traded on the dark Web due to the value of identities that are typically not monitored.
- **Identity Theft Insurance:** You are insured against certain reimbursable expenses in the event that your identity is compromised with a \$1,000,000 insurance policy that has been issued to CSID (subject to the terms and exclusions in the policy).
- **Identity Restoration:** Work with a certified identity theft restoration specialist, who will work on your behalf to restore your identity and let you get on with your life.

### Fraud Alerts

| <u>Equifax</u>   | <u>Experian</u>  | <u>TransUnion</u>  |
|--|--|--|
| P.O. Box 740241  | P.O. Box 2002  | P.O. Box 6790  |
| Atlanta GA 30374   | Allen, TX 75013  | Fullerton, CA 92834  |
| 1-877-478-7625   | 1-888-397-3742   | 1-800-680-7289   |
| <a href="http://www.fraudalerts.equifax.com">www.fraudalerts.equifax.com</a> | <a href="http://www.experian.com">www.experian.com</a> | <a href="http://www.transunion.com">www.transunion.com</a> |

In addition to completing the CSID Protector enrollment, we strongly suggest that you contact the fraud departments of any one of the three major credit-reporting agencies and let them know you may be a potential victim of identity theft. The agency you choose to notify will contact the other two on your behalf. Through that process, a "fraud alert" will automatically be placed in each of your three credit reports to notify creditors not to issue new credit in your name without gaining your permission.

We also encourage you to carefully review your credit report(s). Look for accounts you did not open and inquiries from creditors that you did not initiate. Also review your personal information for accuracy, such as home address and Social Security Number. If you see anything you do not understand or that is inaccurate, call the credit-reporting agency at the telephone number on the report. If you find suspicious activity on your credit reports or bank account, call your local police or sheriff's office and file a police report of identity theft. Get a copy of the police report. You may need copies of the police report to clear your personal records.

You have the right to obtain a police report if you are the victim of identity theft. You also have the right to place a security freeze on your credit report by contacting the credit bureaus listed above. A security freeze is intended to

prevent credit, loans and services from being approved in your name without your consent. To place a security freeze on your credit report, you may be able to use an online process, an automated telephone line or a written request. The following information must be included when requesting a security freeze (note that to establish a credit freeze for a spouse, that spouse's information will also need to be provided): (1) full name with middle initial and any suffixes, (2) Social Security Number, (3) date of birth, (4) current address and any previous address in the last five years and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or a bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address and contain the date of issue. The consumer reporting agency may charge you a fee to place or remove a freeze. However, if you are a victim of identity theft or the spouse of an identity theft victim and you have submitted a valid police report relating to the identity theft incident to the consumer reporting agency, there is no fee.

**Learn about the FTC's identity theft programs at <http://www.ftc.gov/bcp/edu/microsites/idtheft>, contact the Federal Trade Commission's toll-free Identity Theft helpline: 1-877-ID-THEFT (1-877-438-4338); TTY: 1-866-653-4261 or write to the FTC at Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington D.C., 20580. You should also report any actual or suspected identity theft to law enforcement, including the FTC.**

For residents of Iowa: In addition to contacting local law enforcement or the FTC, you may also contact the Iowa Attorney General's office to report suspicious incidents of identity theft at Iowa Attorney General, 1305 E. Walnut Street, Des Moines, IA 50319, 1.515.281.5164; <http://www.iowaattorneygeneral.gov>.

For residents of Maryland: In addition to contacting the FTC, Equifax, Experian or Transunion to obtain more information about the steps you can take to avoid identity theft, you may also contact the Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, 1.888.743.0023; [www.oag.state.md.us](http://www.oag.state.md.us).

For residents of North Carolina: In addition to contacting the FTC, Equifax, Experian or Transunion to obtain more information about the steps you can take to avoid identity theft, you may also contact the North Carolina Office of the Attorney General, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699, 1.919.716.6400; [www.hcdoj.gov](http://www.hcdoj.gov).